DATA PROTECTION ACT 2018
(PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

DATED: 19 FEBRUARY 2024

To: Serco Leisure Operating Limited

Of: Serco House, 16 Bartley Wood Business Park, Bartley Way, Hook, Hampshire, RG27 9UZ

1. Serco Leisure Operating Limited (Companies House number **04687478**) (**Serco**) is a "controller" as variously defined in section 3(6) of the Data Protection Act 2018 ("**DPA**") and Article 4(7) of the UK General Data Protection Regulation ("**UK GDPR**"). In relation to some of the processing that is relevant for this Notice, Serco acts as a joint controller, as further described below.

2. The Information Commissioner ("the **Commissioner**") issues this Enforcement Notice to Serco under section 149(2)(a) and (c) of the DPA. The Notice is in relation to contraventions of Articles 5(1)(a), 6 and 9 of the UK GDPR.

3. This Notice explains the Commissioner's decision. The steps that Serco is required to take are set out in Annex 1.

4. The Commissioner has previously served Serco with a Preliminary Enforcement Notice ("the **PEN**") dated 7 November 2023. Serco provided written representations, on behalf of itself and others with whom it acts as joint controller (as described below) ("the

Representations") in response to the PEN on 5 December 2023. The Commissioner has taken the Representations into account when deciding to issue this Notice and refers to the Representations below when appropriate.

Legal framework for this Notice

5. The DPA contains various enforcement powers in Part 6, which are exercisable by the Commissioner.

6. Section 149 of the DPA 2018, materially provides:

"(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or
(b) to refrain from taking steps specified in the notice, or both (and see also sections 150 and 151).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the [UK] GDPR… (principles of processing);
(b) …; and
(c) a provision of Articles 25 to 39 of the [UK] GDPR… (obligations of controllers and processors)

…

(6) An enforcement notice given in reliance on subsection (2)… may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure."

7. Section 150 of the DPA, materially provides:

"(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

…

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).”

8. Article 4(14) of the UK GDPR sets out a definition of “biometric data” as follows:

“personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”.

9. Article 26(1) of the UK GDPR provides that:

“*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by domestic law. The arrangement may designate a contact point for data subjects.”*

10. By reason of Article 5(1), the UK GDPR includes the following requirement:

“5(1)(a) personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”)”

11. Article 6 of the UK GDPR makes provision for the lawfulness of processing. In particular for the purposes of this Notice, it provides that:

"Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

…

…

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…"

12. Article 9(1) of the UK GDPR, provides:

"(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

13. Article 9(2) of the UK GDPR materially provides:

"Paragraph 1 shall not apply if one of the following applies:

…

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

…"

14. Schedule 1, Part 1 Paragraph 1 of the DPA makes further provision for the application of Article 9(2)(b) of the UK GDPR, as follows:

"(1) This condition is met if -

(a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and

(b) when the processing is carried out the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule)"

15. Schedule 1, Part 4, Paragraph 39 of the DPA provides that:

"The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition [in Part 1, 2 or 3 of the Schedule which requires the controller to have an appropriate policy document in place] *if the controller has produced a document which –*

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR…, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained."

Background

16. Serco is a large multinational organisation specialising in the delivery of public services, including, for the purposes of this Notice, leisure services. Serco operates leisure facilities on behalf of community leisure trusts, local authorities and Sport England.

17. This Notice concerns 38 Serco-operated leisure facilities where processing of biometric data (as defined at Article 4(14) of the UK GDPR) is taking place (the **Relevant Facilities**).

18. Of the 38 Relevant Facilities, 37 are located in the UK and one in Jersey.

19. As part of the operation of the Relevant Facilities, Serco runs the day-to-day management of the centres' employees. Some employees are employed by Serco, whilst others may be employed by the community leisure trust for that Relevant Facility.

20. For five of the Relevant Facilities, Serco is the sole controller in relation to the processing of biometric data. At 32 of the Relevant Facilities, Serco is a joint controller with the leisure trust for that Relevant Facility (each known as a **Trust**). At the Relevant Facility

in Jersey, Serco is a joint controller with Serco (Jersey) Limited (**Serco Jersey**) as defined in Article 26 (1) of the UK GDPR.

21. Serco processes biometric data for the purpose of monitoring employee attendance. Facial recognition technology (**FRT**) is in use at all 38 Relevant Facilities. At two of the Relevant Facilities, both FRT and fingerprint scanning technology are in use.

22. Serco began processing biometric data at Relevant Facilities in May 2017, when Serco took over operation of a site that was already using an FRT system. Following a trial in 2018, biometric technology was rolled out at the other Relevant Facilities throughout 2019 and in November 2022.

23. The FRT and fingerprint scanning systems are provided to Serco by SWT Software Limited, trading as ShopWorks, which acts as a processor (as defined at Article 4(8) of the UK GDPR), on behalf of Serco.

24. On 2 December 2019, a referral to the Information Commissioner's Office Civil Investigations department was made after an employee of the Information Commissioner's Office observed FRT in use at one of the Relevant Facilities. The Commissioner subsequently opened an investigation into Serco's processing of biometric data (**Investigation**).

25. It is also relevant that Serco has received one complaint in relation to the use of FRT at one of the Relevant Facilities. The Commissioner has also received one complaint relating to the processing using FRT.

26. The Investigation found the following material facts:

a) Serco was using, and continues to use, FRT to collect special category personal data for the purpose of employment attendance checks and subsequent payment for employees' time worked.

b) The FRT system works by registering employees onto an FRT scanner, by having their photograph taken by the scanner three times. The scanner uses the images to create a biometric map based on the employee's facial features. This map is encrypted and held within the scanner itself, which also holds a record of the employee's name and staff number. When an employee activates the scanner, it captures an image of the employee, converts this into a biometric map and attempts to match this against the maps stored on the device. If the scanner finds a match, it passes the employee's staff number, match time and location to the ShopWorks server and deletes the captured image. If the scanner does not find a match, it deletes the captured image. A manager reviews and approves all employee hours recorded by the scanner at the end of each day and these can then be viewed on an employee self-service portal. Serco did not provide a detailed description of the fingerprint scanning systems in operation at two of the Relevant Facilities.

c) Serco introduced biometric technology at the Relevant Facilities because it considered that previous systems were open to abuse by employees. Serco explained to the Commissioner in its responses to enquiries and Representations that manual sign-in sheets were prone to human error and abused by a minority of employees. Serco also explained that radio-frequency identification cards were used inappropriately by employees at one Relevant Facility, where cards were shared and kept in

communal areas. Serco did not provide any figures or evidence indicating the number of employees "abusing the system".

d) Serco considers that using biometric technology is the only way to prevent these abuses of the system from happening in practice. Serco advised the Commissioner that: *"biometrics is the sole technology capable of eliminating buddy punching and falsified time cards"* and that biometric solutions are *"more accurate and secure than cards or keys, because a fingerprint or face scan cannot be lost, stolen or (easily) replicated."*

e) Serco has produced both a data protection impact assessment (**DPIA**) and a legitimate interests assessment (**LIA**) for the processing. The LIA was conducted after the roll-out of the technology and following contact from the Commissioner. Serco has identified the lawful bases for the processing as Article 6(1)(b) of the UK GDPR (contractual necessity) and Article 6(1)(f) of the UK GDPR (legitimate interests). Serco has identified the relevant processing condition for special category personal data as Article 9(2)(b) of the UK GDPR (employment, social security and social protection), on the basis that Serco needs to process attendance data to comply with a number of regulations, such as working time regulations, national living wage, right to work rules and tax/accounting regulations.

f) Serco advised the Commissioner that if an employee raises concerns regarding the use of biometric technology, and does not wish to use it, an alternative process will be considered. Serco stated that an alternative process has been used once where the scanner was unable to recognise an employee, but have not specified what alternative process would be available

(though this could include the use of a pass or card). Serco's original LIA (dated 24 March 2020) stated that *"an opt out would be unsuitable"* for the processing. This was updated on 28 April 2021 to confirm that an alternative process would be considered if an employee were to raise concerns. However, this policy was not in place for some time whilst biometric technology was in use.

g) Taking into account documents and responses provided to the Commissioner by Serco, the information given to employees is not clear as to whether they are able to object to the processing in practice. Serco's Leisure Standard Operating Procedure (**LSOP**) states that: *"All employees based on a Contract are expected to use the ShopWorks platform"*. The LSOP further outlines the consequences of refusing to use the system (rather than objecting to its use): *"All staff are … required to comply to use of tools in place to accurately enable capture of time and attendance. Non-compliance or refusal to enrol may lead to an investigation and it may escalate to disciplinary action for failure to follow a reasonable line management instruction and operating requirement."*

h) When one affected data subject complained to Serco about the use of FRT, Serco did not offer an alternative and instead offered to arrange a meeting between the affected data subject and a ShopWorks representative to discuss privacy concerns. The data subject was informed that they would *"be required to use the ShopWorks… system"* on their return to work.

i) As of 23 November 2022, Serco provided responses to the Commissioner's enquiries explaining that, at that date, 2,283

data subjects were affected by the use of biometric technology at the Relevant Facilities. 2,068 of these data subjects are subject to the use of FRT and 215 of the data subjects are employees at the two Relevant Facilities where both FRT and fingerprint scanning are in use.

j) Serco explained in its Representations that, since the FRT system has been in place, approximately 7 million biometric scans have taken place.

The contravention

27. In light of the above and on consideration of the Representations made by Serco, the Commissioner finds that Serco has contravened Articles 5(1)(a), 6 and 9 of the UK GDPR in that it in its role as a controller, it has failed to, establish a lawful basis and special category personal data processing condition for the processing of biometric data as required by Articles 5(1)(a), 6 and 9.

Article 6 – lawful basis for processing

28. Serco purports to rely on Article 6(1)(b) (contractual necessity) and Article 6(1)(f) (legitimate interests).

29. Regarding Serco's reliance on Article 6(1)(b), Serco states that the processing of attendance data is necessary to ensure employees are paid correctly for the time they have worked. Although recording attendance times may be necessary for Serco to fulfil its obligations under employment contracts, it does not follow that the processing of biometric data is necessary to achieve this purpose. The processing of biometric data cannot be considered "necessary"

when less intrusive means could be used to verify attendance. The less intrusive means of recording attendance times that are available to Serco include using radio-frequency identification cards or fobs, or manual sign-in and sign-out sheets. Serco has failed to demonstrate why these less intrusive methods are not appropriate. Despite Serco's assertions that these methods are open to abuse, Serco has not been able to provide evidence of widespread abuse, nor why other methods, such as disciplinary action against employees found to be abusing the system, have not been considered to be appropriate. Serco cannot rely on Article 6(1)(b) to process biometric data, as the availability of less intrusive methods of recording attendance data means that this processing is not necessary in order for Serco to fulfil its employment contracts.

30. Regarding Serco's reliance on Article 6(1)(f), Serco identifies its legitimate interests as:

    a) *"to ensure Serco are paying staff members the correct salary for the time worked;*
    b) *"to support our administrative and business functions."*

31. Legitimate interests will not apply if a controller can reasonably achieve the same result in another less intrusive way. As described above, Serco has not provided enough information to support its argument that eliminating abuse of the attendance monitoring system is a necessity, rather than simply a further benefit to Serco. There is a lack of evidence from Serco of any consideration of alternative means of handling such abuse, for example taking disciplinary action against the individuals responsible (which Serco acknowledges constitute only a minority of employees). Whilst

"necessity" does not mean that the processing must be "absolutely essential", it must be more than just "useful" and be a targeted and proportionate way of achieving the purpose. In this case, the use of biometric technology to monitor attendance is not a targeted means of paying employees correctly or a proportionate method of overcoming the issue of a small number of employees having abused previous systems.

32. In applying the balancing test required to rely on legitimate interests, Serco has failed to give appropriate weight to the intrusive nature of biometric processing or the risks to data subjects.

33. Serco cannot rely on Article 6(1)(f) as it has failed to demonstrate the necessity of the processing or give appropriate weight to the interests of data subjects when conducting the balancing test. Less intrusive means of achieving the results are available. Legitimate interests is not an appropriate lawful basis as:

a) The processing has a substantial privacy impact. Biometric data is inherently sensitive due to its uniqueness to the person to whom it relates, and the increased potential for harm if that data is compromised (for example, allowing access to further sensitive and private data such as bank accounts). In this case, employees are required to provide biometric data that will be processed regularly and systematically as part of their employment. This is a regular intrusion into employees' privacy, over which they have no, or minimal, control.
b) Employees were not given clear information about how they could object to the processing, or about any alternative methods of monitoring attendance that did not involve intrusive processing.

c) There is an imbalance of power between Serco, as employer, and the employees. This means that even if employees had been informed that they could object to the processing, the Commissioner considers that they may not have felt able to do so.

Article 9 – special category personal data processing condition

34. Serco sought to rely on Article 9(2)(b) as its processing condition for processing special category personal data, however Serco initially failed (including in its DPIA) to identify the specific obligation or right conferred by law. Serco's Representations identified the relevant laws in this context as:
    a) Section 9 of the Working Time Regulations 1998, which requires employers to keep adequate records of timekeeping; and
    b) the Employment Rights Act 1996 relating to the correct payment of wages, including the right under Section 13 of that Act for the worker not to suffer unauthorised deductions from their wages.

35. However, these were not identified at the time Serco began processing data using the FRT system, nor did Serco refer to these laws in its responses to enquiries during the Commissioner's investigation. The Article 9(2)(b) processing condition does not cover processing to meet purely contractual employment rights or obligations.

36. Serco has not produced an appropriate policy document as required by Schedule 1, Paragraph 1(1)(b) of the DPA.

37. Serco has also, as described above, failed to demonstrate that the processing of biometric data is "necessary" for Serco to process

special category data for the purpose of employment attendance checks or to comply with the relevant laws identified in the Representations.

38. Serco cannot rely on Article 9(2) to process biometric data using FRT or fingerprint scanning technology.

Article 5(1)(a) – lawful, fair and transparent processing

39. In failing to establish a lawful basis and processing condition under Articles 6 and 9 respectively, Serco has failed to comply with its obligations under Article 5(1)(a) to process the biometric data lawfully. The fact that the processing has been taking place since May 2017 and has affected a significant number of data subjects (at least 2,283) increases the seriousness of the infringement.

40. The Commissioner also finds that Serco has failed to process personal data fairly in accordance with its Article 5(1)(a) obligations. The processing of biometric data is highly intrusive and has the potential to cause distress to data subjects. Although Serco has stated that alternative mechanisms for employees to log their attendance will be available, this is not clearly brought to employees' attention, even when an employee has complained. In fact, the LSOP explains that employees are "expected" to use the biometric technology, that the use of the biometric technology is a requirement and that employees could be subject to disciplinary action if they refuse to use it. The LSOP does not set out how data subjects could object to any processing.

41. The Commissioner also considers that, due to the imbalance of power between Serco (as employer) and its employees (and those of the relevant Trusts, where applicable), it is unlikely that an

employee would feel able to object to this processing. It is also not made clear to data subjects how they can make such an objection.

Are the contraventions identified deliberate or negligent?

42. Although the use of FRT and processing of biometric data are deliberate, the Commissioner considers that the resulting infringements are negligent. Serco appears to have sought to comply with data protection legislation in its deployment of biometric technology, but its failure to meet these requirements indicates a lack of understanding of the UK GDPR.

43. The Trusts, as joint controllers, are also considered to have been negligent in their decision to sign off on the implementation of technology that does not meet the requirements of the legislation. Each Trust is the subject of a separate Enforcement Notice in relation to its role in the processing of biometric data.

Issue of the Notice

44. The Commissioner has considered, as he is required to do under section 150(2) the DPA when considering whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner has decided that the processing of biometric data in these circumstances is either causing and/or likely to cause distress to data subjects. The processing of biometric data is, by nature, highly intrusive. Due to the imbalance of power between Serco (as employer) and its (and the relevant Trust's) employees, the relevant data subjects are in a vulnerable position. There is evidence that distress has been caused to data subjects, including

the receipt by Serco and the ICO of a complaint relating to the processing.

45. Having regard to the contraventions, Serco's responses to the Commissioner's enquiries, Serco's Representations and the duration of the infringement, the Commissioner considers that an Enforcement Notice would be a proportionate regulatory step to bring Serco into compliance. The Commissioner requires Serco to take the steps specified in Annex 1 of this Notice.

Consequences of failing to comply with an Enforcement Notice

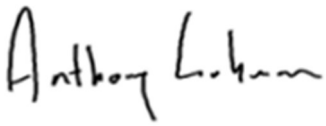
46. If a person fails to comply with an Enforcement Notice, the Commissioner may serve a penalty notice on that person under section 155(1)(b) of the DPA 2018, requiring payment of an amount up to £17,500,00 or 4% of an undertaking's total annual worldwide turnover, whichever is the higher.

Right of Appeal

47. By virtue of section 162(1)(c) of the DPA 2018, there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights), part of the General Regulatory Chamber. Information about appeals is set out in the attached Annex 2.

Dated the 19th day of February 2024

Signed:



Anthony Luhman
Temporary Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE ENFORCEMENT NOTICE

By no later than the date three months from the date of the Enforcement Notice Serco shall take the following steps:

1. Cease all processing of biometric data for the purpose of employment attendance checks from all Relevant Facilities (and not implement biometric technology at any further facilities).

2. Destroy all biometric data and all other personal and special category data that Serco is not legally obliged to retain, including any such data stored by, or on behalf of Serco (including instructing SWT Software Limited to delete any such data held on behalf of Serco).

ANNEX 2

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1)(c) of the DPA gives any person upon whom an Enforcement Notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the "**Tribunal**") against the Enforcement Notice.

2. If you decide to appeal and if the Tribunal considers:-

    a. that the Enforcement Notice against which the appeal is brought is not in accordance with the law; or

    b. to the extent that the Enforcement Notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

    the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

    General Regulatory Chamber
    HM Courts & Tribunals Service
    PO Box 9300
    Leicester
    LE1 8DJ

Telephone: 0203 936 8963

Email: grc@justice.gov.uk

4. Any notice of appeal should be served on the Tribunal within 28 days of the date on which the Enforcement Notice was sent.